(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号

特開平9－46330

(43)公開日　平成９年(1997)２月14日

(51)Int.Cl.[6]		識別記号	庁内整理番号	ＦＩ		技術表示箇所
Ｈ０４Ｌ	9/08			Ｈ０４Ｌ	9/00	６０１Ａ
Ｇ０６Ｆ	13/00	３５１	9460－5E	Ｇ０６Ｆ	13/00	３５１Ｇ
Ｇ０９Ｃ	1/00	６３０	7259－5J	Ｇ０９Ｃ	1/00	６３０Ａ
			7259－5J			６３０Ｅ
		６６０	7259－5J			６６０Ｅ

審査請求　未請求　請求項の数３　ＯＬ　（全 16 頁）　最終頁に続く

(21)出願番号　特願平7－193447

(22)出願日　平成７年(1995)７月28日

(71)出願人　000003078
株式会社東芝
神奈川県川崎市幸区堀川町72番地

(72)発明者　室田　真男
神奈川県川崎市幸区小向東芝町１番地　株式会社東芝研究開発センター内

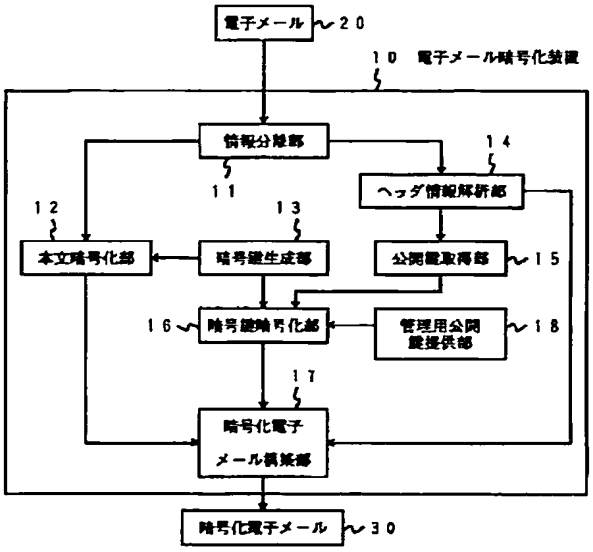
(74)代理人　弁理士　鈴江　武彦

(54)【発明の名称】　電子メール暗号化装置及び電子メール転送装置

(57)【要約】

【課題】　電子メールの送信者及び受信者以外の第三者が暗号化電子メールに関する情報管理を行うことができる電子メール暗号化装置を提供すること。

【解決手段】　所定の暗号鍵を用いて共通鍵暗号方式により暗号化した電子メールの本文に、該電子メールの送信者と受信者用の夫々の公開鍵を用いて公開鍵暗号方式により暗号化した該所定の暗号鍵を付加して暗号化電子メールを構築する電子メール暗号化装置において、予め定められた前記電子メールの受信者及び送信者以外の第三者の公開鍵を用いて前記所定の暗号鍵を暗号化する手段と、前記第三者の公開鍵により暗号化した前記所定の暗号鍵を前記電子メールに付加する手段とを備えたことを特徴とする。



1

【特許請求の範囲】
【請求項１】所定の暗号鍵を用いて共通鍵暗号方式により暗号化した電子メールの本文に、該電子メールの送信者と受信者用の夫々の公開鍵を用いて公開鍵暗号方式により暗号化した該所定の暗号鍵を付加して暗号化電子メールを構築する電子メール暗号化装置において、
予め定められた前記電子メールの受信者及び送信者以外の第三者の公開鍵を用いて前記所定の暗号鍵を暗号化する手段と、
前記第三者の公開鍵により暗号化した前記所定の暗号鍵を前記電子メールに付加する手段とを備えたことを特徴とする電子メール暗号化装置。
【請求項２】電子メールの転送を行う電子メール転送装置において、
転送対象とされた電子メールの種類を判別する手段と、
判別された電子メールの種類に応じて該電子メールの転送の可否を判断する手段とを備えたことを特徴とする電子メール転送装置。
【請求項３】転送可能と判断された電子メールが管理用の暗号鍵情報を含むものである場合、この暗号化電子メールから該管理用の暗号鍵情報を取り除く手段をさらに備えたことを特徴とする請求項２に記載の電子メール転送装置。
【発明の詳細な説明】
【０００１】
【発明の属する技術分野】本発明は、電子メール暗号化装置及び電子メール転送装置に関する。
【０００２】
【従来の技術】コンピュータネットワークの普及に伴い、電子メールが広く利用されるようになってきた。さらには、秘匿すべき情報を電子メールとして転送したいという要求から、電子メール暗号化装置が提供されている。
【０００３】暗号化電子メール装置は、ＰＥＭ（Ｐｒｉｖａｃｙ　Ｅｎｈａｎｃｅｄ　Ｍａｉｌ）やＰＧＰ（Ｐｒｅｔｔｙ　Ｇｏｏｄ　Ｐｒｉｖａｃｙ）において実現されている。以下に、電子メールを暗号化する手順を示す。
【０００４】まず、共通鍵暗号方式用の暗号鍵を生成し、その暗号鍵を用いて共通鍵暗号方式により電子メール本文を暗号化する。次に、本文の暗号化に用いた暗号鍵を、電子メールの送信者と受信者のそれぞれの公開鍵を用いて公開鍵暗号化方式により暗号化して、送信者用暗号鍵情報と受信者用暗号鍵情報を作成する。受信者が複数いる場合は、それぞれの受信者に対する暗号鍵情報を作る。そして、暗号化された本文と所定数の受信者用暗号鍵情報と送信者用暗号鍵情報が暗号化電子メールとして送られる。
【０００５】このようにして暗号化された暗号化電子メールを受信者や送信者が読むときは、まず、自分用に付与された暗号鍵情報を自分の秘密鍵を用いて復号して暗号鍵を得る。ここで用いる秘密鍵は、暗号鍵情報を作るときに用いられた公開鍵の対になっているものである。その秘密鍵を持っている者のみが、暗号鍵情報を復号して暗号鍵を得ることができる。暗号鍵を得た後は、共通鍵暗号方式を用いて本文を復号し読むことができる。

2

【０００６】ところで、企業などにおいては、電子メールにより企業外部に秘密情報を漏洩されるのを防ぐために、電子メールの内容に関する情報管理を行ないたい要求がある。
【０００７】本文が暗号化されていない電子メールの場合は、その内容は送信者と受信者以外でも読むことができるので、電子メール転送装置などにおいて電子メールのコピーをログとして保存することにより情報管理を行なうことができる。
【０００８】ところが、従来の暗号化電子メールにおいて暗号化された本文を復号することができるのは、電子メールの送信者と受信者のみである。従って、電子メール転送装置において保存されたログを見ても、電子メール管理者は暗号化電子メールの内容を読むことができないため、情報管理をすることができないという問題点があった。
【０００９】また、従来の電子メール転送装置は、電子メールの転送を要求されると、その電子メールのヘッダから受信者を読取って転送を行なうだけであった。従って、機密性の高い情報を持つ暗号化電子メールでも、要求があれば転送してしまうので、誤転送などのおそれがあり、セキュリティー上の大きな問題が残されていた。
【００１０】
【発明が解決しようとする課題】従来の電子メール暗号化装置では、これにより暗号化された電子メールの内容を電子メールの管理者が読むことができないため、情報管理をすることができないという問題点があった。
【００１１】また、従来の電子メール転送装置では、電子メールを無条件に転送していたので、セキュリティー上の問題点が残されていた。本発明は、上記事情に考慮してなされたものであり、電子メールの送信者及び受信者以外の第三者が暗号化電子メールに関する情報管理を行うことができる電子メール暗号化装置を提供することを目的とする。また、本発明は、暗号化電子メールに関する転送制御を行うことができる電子メール転送装置を提供することを目的とする。
【００１２】
【課題を解決するための手段】本発明（請求項１）は、所定の暗号鍵を用いて共通鍵暗号方式により暗号化した電子メールの本文に、該電子メールの送信者と受信者用の夫々の公開鍵を用いて公開鍵暗号方式により暗号化した該所定の暗号鍵を付加して暗号化電子メールを構築する電子メール暗号化装置において、予め定められた前記電子メールの受信者及び送信者以外の第三者の公開鍵を

用いて前記所定の暗号鍵を暗号化する手段と、前記第三者の公開鍵により暗号化した前記所定の暗号鍵を前記電子メールに付加する手段とを備えたことを特徴とする。

【００１３】本発明（請求項２）は、電子メールの転送を行う電子メール転送装置において、転送対象とされた電子メールの種類を判別する手段と、判別された電子メールの種類に応じて該電子メールの転送の可否を判断する手段とを備えたことを特徴とする。

【００１４】本発明（請求項３）は、上記発明（請求項２）の電子メール転送装置において、転送可能と判断された電子メールが管理用の暗号鍵情報を含むものである場合、この暗号化電子メールから該管理用の暗号鍵情報を取り除く手段をさらに備えたことを特徴とする。

【００１５】また、本発明に係る電子メール暗号化方法は、電子メールの本文を所定の暗号鍵を用いて共通鍵暗号方式により暗号化するステップと、該所定の暗号鍵を該電子メールの送信者用の公開鍵を用いて公開鍵暗号方式により暗号化するステップと、該所定の暗号鍵を該電子メールの受信者用の公開鍵を用いて公開鍵暗号方式により暗号化するステップと、予め定められた前記電子メールの受信者及び送信者以外の第三者の公開鍵を用いて前記所定の暗号鍵を暗号化するステップの４つのステップを所定の順番にあるいは並行して行なった後、暗号化された前記本文に前記夫々の公開鍵で暗号化された公開鍵を付加して暗号化電子メールを構築することを特徴とする。

【００１６】また、本発明に係る電子メール転送方法は、転送対象とされた電子メールの種類を判別し、判別された電子メールの種類に応じて該電子メールの転送の可否を判断し、転送可能と判断された電子メールを転送することを特徴とする。

【００１７】また、本発明に係る電子メール転送方法は、転送対象とされた電子メールの種類を判別し、判別された電子メールの種類に応じて該電子メールの転送の可否を判断し、転送可能と判断された電子メールが管理用の暗号鍵情報を含むものである場合、転送に先だってこの暗号化電子メールから該管理用の暗号鍵情報を取り除き、転送可能と判断された電子メールを転送することを特徴とする。

【００１８】（作用）本発明（請求項１）では、電子メール暗号化装置が、電子メール本文の暗号化に用いた暗号鍵を電子メールの受信者と送信者以外の第三者の公開鍵により暗号化し、電子メールに付加する。その結果、本発明の電子メール暗号化装置により暗号化された電子メールは、受信者用、送信者用、第三者用のそれぞれの公開鍵で暗号化された暗号鍵情報が付けられる。したがって、この暗号化された電子メールを復号できるのは、受信者、送信者、そして第三者となる。ここで、第三者を電子メール情報管理者とすると、該管理者は電子メールの内容検査などの情報管理を行うことができる。

【００１９】本発明（請求項２）では、入力された電子メールの種類を判別し、その結果に応じて該電子メールの転送の可否を判断する。例えば、電子メールが暗号化されていないものか、暗号化されたものかを判別する。さらには、暗号化電子メールについては、管理用暗号鍵情報を含むものであるか否かなど、種類をより細分化することもできる。そして、暗号化されていない電子メールだけ転送可、あるいは暗号化された電子メールについても、管理用暗号鍵情報を含む暗号化された電子メールは転送可、管理用暗号鍵情報を含まない暗号化された電子メールは転送不可、といったような判断を行う。そして、転送可能と判断された電子メールだけ転送する。

【００２０】例えば、該電子メール転送装置を企業の内部と外部との境界に置くことにより、企業が情報管理できる電子メールのみを外部に転送する、といったことを行うことができる。

【００２１】本発明（請求項３）では、上記発明（請求項２）の電子メール転送装置において、管理用の暗号鍵情報を含む暗号化電子メールから該暗号鍵情報を取り除く手段をさらに設けたので、メール送信者と受信者にとって本来不要である管理用の暗号鍵情報を除去することができる。

【００２２】

【発明の実施の形態】以下、図面を参照しながらこの発明の実施の形態を説明する。図１に、本発明の第１の実施の形態に係る電子メール暗号化装置の基本構成を示す。電子メール暗号化装置１０は、電子メール（図中２０）を入力し、これを暗号化し、暗号化電子メール（図中３０）として出力するものであり、情報分離部１１、本文暗号化部１２、暗号鍵生成部１３、ヘッダ情報解析部１４、公開鍵取得部１５、暗号鍵暗号化部１６、暗号化電子メール構築部１７、管理用公開鍵提供部１８を備えている。

【００２３】図２は、暗号化の対象となる電子メールの基本的構造を示す。電子メール（２０）は、ヘッダ情報部と本文（２３）からなる。図２の例では、ヘッダ情報として送信者を表す送信者情報（２１）と受信者を列記した受信者情報（２２）が示されている。図２の例では、この電子メール（２０）は送信者Ｓから受信者Ａおよび受信者Ｂに宛てたものであることを示している。

【００２４】図３には、電子メール暗号化装置１０による電子メール暗号化処理の手順の一例を示す。以下、図３を参照しながら、電子メール暗号化処理を説明する。

【００２５】電子メール暗号化装置１０に入力された電子メール（２０）は、情報分離部１１により、送信者情報や受信者情報を含むヘッダ情報と本文に分けられる（ステップＳ１）。本文は本文暗号化部１２に、ヘッダ情報はヘッダ情報解析部１４に夫々送られる。

【００２６】暗号鍵生成部１３は、本文の暗号化に用いる共通鍵暗号方式の暗号鍵を生成する（ステップＳ

２）。生成された暗号鍵は、本文暗号化部１２と暗号鍵暗号化部１６に渡される。

【００２７】本文暗号化部１２は、該暗号鍵を用いて共通鍵暗号方式により本文を暗号化する（ステップＳ３）。共通鍵暗号方式としては、従来知られている方式、例えばＤＥＳ（ＤａｔａＥｎｃｒｙｐｔｉｏｎ　Ｓｔａｎｄａｒｄ）方式などを用いる。

【００２８】暗号化された本文は、暗号化電子メール構築部１７に渡される。ヘッダ情報解析部１４は、ヘッダ情報の送信者情報（２１）から送信者を、受信者情報（２２）から受信者を解析する（ステップＳ４）。そして、この解析結果（図２の場合、送信者Ｓ／受信者Ａ／受信者Ｂ）を公開鍵取得部１５に渡す。また、ヘッダ情報は、暗号化電子メール構築部１７に送られる。

【００２９】公開鍵取得部１５は、ヘッダ情報解析部１４から送信者及び受信者の情報を渡されると、送信者及び受信者それぞれの公開鍵を取得する（ステップＳ５）。公開鍵の取得方法としては、例えば、ローカルにデータベースを持っていてもよいし、公開鍵を提供するサーバからネットワーク経由で取得してきてもよい。取得された公開鍵は、暗号鍵暗号化部１６に渡される。

【００３０】管理用公開鍵提供部１８は、電子メール管理用にあらかじめ定められた公開鍵を暗号鍵暗号化部１６に渡す。管理用の公開鍵は、管理用公開鍵提供部１８があらかじめ保有していてもよいし、別の場所から取得してきてもよい（ステップＳ７）。

【００３１】ただし、入力電子メール（２０）のヘッダ情報の受信者情報に管理者が書込まれていた場合には、上記のステップＳ５の処理で管理用公開鍵は入手されているので、管理用公開鍵提供部１８から入手を省略してよい（ステップＳ６）。

【００３２】暗号鍵暗号化部１６は、暗号鍵生成部１３で生成された前記暗号鍵を、公開鍵取得部１５から受け取った受信者の公開鍵および送信者の公開鍵、ならびに管理用公開鍵提供部１８から受け取った管理用の公開鍵を用いて、それぞれ公開鍵暗号方式により暗号化し、受信者用暗号鍵情報、送信者用暗号鍵情報、および管理用暗号鍵情報を作成する（ステップＳ８）。上記公開鍵暗号方式は、従来知られている方式、例えばＲＳＡ方式などを用いる。ここで生成された各暗号鍵情報は、暗号化電子メール構築部１７に渡される。

【００３３】暗号化電子メール構築部１７は、本文暗号化部１２より渡された暗号化された本文、暗号鍵暗号化部１６より渡された受信者用暗号鍵情報、送信者用暗号鍵情報および管理用暗号鍵情報、ならびにヘッダ情報解析部１４より渡されたヘッダ情報を用いて、暗号化電子メール（３０）を構築して（ステップＳ９）、出力する。

【００３４】図４は、図２の電子メール（２０）を上記のようにして暗号化した暗号化電子メール（３０）の構造を示す。暗号化電子メール（３０）は、送信者情報（２１）および受信者情報（２２）からなるヘッダ情報、受信者Ａ用暗号鍵情報（３３）、受信者Ｂ用暗号鍵情報（３４）、送信者Ｓ用暗号鍵情報（３５）および管理用暗号鍵情報（３６）からなる電子メール本文暗号鍵情報、ならびに暗号化本文（３７）から構成される。

【００３５】送信者情報（２１）と受信者情報（２２）は、図２の電子メールと同じもの（平文）である。受信者Ａ用暗号鍵情報（３３）には受信者Ａの公開鍵、受信者Ｂ用暗号鍵情報（３４）には受信者Ｂの公開鍵、送信者Ｓ用暗号鍵情報（３５）には送信者Ｓの公開鍵、管理用暗号鍵情報（３６）には管理用の公開鍵を用いて、それぞれ本文の暗号鍵が公開鍵暗号方式により暗号化された情報が記述されている。

【００３６】電子メール受信者は、自分用の暗号鍵情報を自分が保有する秘密鍵により復号化して電子メール本文の暗号鍵を得ることができ、該暗号鍵を用いて電子メール本文を復号化することができる。ここで、各暗号鍵情報を復号して本文の暗号鍵を得ることができるのは、それぞれの公開鍵に対応する秘密鍵を保有する者だけである。

【００３７】従って、図１の電子メール暗号化装置１０により暗号化された暗号化電子メール（３０）を復号して読むことができるのは、電子メール（２０）の送信者、受信者Ａ、受信者Ｂ、そして管理用の秘密鍵を有する管理者だけである。

【００３８】この実施の形態の電子メール暗号化装置１０による暗号化電子メール（３０）は、送信者と受信者以外の第三者である管理者が電子メールを復号できる点に特徴がある。つまり、管理者により暗号化電子メール（３０）の内容検査が可能となり、電子メールの情報管理が可能となる。従って、このような電子メール暗号化装置を、例えば、企業などによる電子メールの情報管理などに用いると効果的である。

【００３９】また、この実施の形態によれば、従来の暗号化電子メールの枠組を大きく変えることなく第三者による暗号化電子メールの情報管理を行うことができるという利点がある。

【００４０】ところで、この実施の形態の電子メール暗号化装置の電子メール暗号化処理の手順は、図３に示したものに限らず、種々変形することができる。図５には、電子メール暗号化装置１０による電子メール暗号化処理の手順の他の例を示す。図３の手順とは、処理の順番が異なっているだけである。すなわち、図３では、暗号化鍵を作成すると（ステップＳ２）、まず、電子メール本文の暗号化を行なったが（ステップＳ３）、図５では、電子メール本文の暗号化（ステップＳ２２）は、暗号化電子メールフォーマットの構築の直前に行なっている（ステップＳ２３）。また、図３では、送信者の判別と受信者の判別（ステップＳ４）をまとめて行ない、送

信者用公開鍵の取得と受信者用公開鍵の取得（ステップＳ５）をまとめて行ない、各公開鍵による本文の暗号鍵の暗号化（ステップＳ８）をまとめて行なっているが、図５では、まず、送信者について、判別（ステップＳ１４）、送信者用公開鍵の取得（ステップＳ１５）、公開鍵による本文の暗号鍵の暗号化（ステップＳ１６）を行ない、次に、受信者について、判別（ステップＳ１８）、送信者用公開鍵の取得（ステップＳ２１）、公開鍵による本文の暗号鍵の暗号化（ステップＳ１６）を行なっている。

【００４１】また、これの他にも、種々の処理手順が考えられるが、当業者であれば容易に修正を施すことができるので、さらなる他の手順の例を一つ一つ説明することは省略する。

【００４２】この実施の形態の電子メール暗号化装置は、ハードウェアで実現することも可能であり、また、上記のような処理内容に相当するプログラムを作成し、これをコンピュータにインストールして実行させる形で実現することも可能である。

【００４３】ここで、比較のために、図１８に従来の電子メール暗号化装置の基本構成を示す。従来の電子メール暗号化装置がこの実施の形態と違う点は、管理用公開鍵提供部１８を持たない点である。従って、暗号鍵暗号化部４６は、電子メールの受信者と送信者の公開鍵のみを受け取り、受信者と送信者に対する暗号鍵情報のみを生成していた。

【００４４】図１９に、従来の電子メール暗号化装置による暗号化電子メールの構造を示す。図に示すように、暗号鍵情報としては受信者用暗号鍵情報（５３，５４）と送信者用暗号鍵情報（５５）のみを含む。従って、該暗号化電子メールを読むことができるのは、送信者と受信者のみであり、第三者である管理者が電子メールの内容を検査するような情報管理を行うことができなかった。

【００４５】次に、図６に、本発明の第２の実施の形態に係る電子メール暗号化装置の基本構成を示す。この電子メール暗号化装置６０は、情報分離部６１、本文暗号化部６２、暗号鍵生成部６３、管理用ヘッダ情報付加部６４、ヘッダ情報解析部６５、公開鍵取得部６６、暗号鍵暗号化部６７、暗号化電子メール構築部６８を備えている。図６の管理用ヘッダ情報付加部６４以外の部分は、基本的には、図１の対応する部分と同様のものである。つまり、図１の構成から管理用公開鍵提供部を省き、代りに管理用ヘッダ情報付加部を設けたものである。

【００４６】また、図１に示す従来の電子メール暗号化装置との違いは、情報分離部６１により分離されたヘッダ情報が、管理用ヘッダ情報付加部６４に渡されその後ヘッダ情報解析部６５に渡される点にある。

【００４７】図７には、電子メール暗号化装置６０による電子メール暗号化処理の手順の一例を示す。以下、図７を参照しながら、電子メール暗号化処理を説明する。

【００４８】電子メール暗号化装置６０に入力された電子メール（２０）は、情報分離部６１により送信者情報や受信者情報を含むヘッダ情報と本文（２３）に分けられる（ステップＳ２１）。そして、本文は本文暗号化部６２に、ヘッダ情報は管理用ヘッダ情報付加部６４に夫々送られる。

【００４９】暗号鍵生成部６３は、本文の暗号化に用いる共通鍵暗号方式の暗号鍵を生成する（ステップＳ２２）。生成された暗号鍵は、本文暗号化部６２と暗号鍵暗号化部６７に渡される。

【００５０】本文暗号化部６２は、該暗号鍵を用いて共通鍵暗号方式により本文を暗号化する（ステップＳ２３）。暗号化された本文は、暗号化電子メール構築部６８に渡される。

【００５１】管理用ヘッダ情報付加部６４は、電子メールの受信者情報にあらかじめ定められている電子メール管理者を加える（ステップＳ２４）。つまり、電子メール（２０）の受信者情報（２２）には、受信者Ａ、受信者Ｂ、管理者が載せられる。ヘッダ情報は、ヘッダ情報解析部６５に渡される。

【００５２】ヘッダ情報解析部６５は、ヘッダ情報の送信者情報（２１）から送信者を解析し、受信者情報から受信者を解析する（ステップＳ２５）。そして、この解析の結果得られた送信者および受信者を公開鍵取得部６６に渡す。この実施の形態では、受信者の中には、前記管理用ヘッダ情報付加部６４で加えられた電子メール管理者が含まれる。なお、ヘッダ情報は、暗号化電子メール構築部６８に送られる。

【００５３】公開鍵取得部６６は、送信者と受信者のそれぞれの公開鍵を取得する（ステップＳ２６）。電子メール（２０）の例では、送信者Ｓ、受信者Ａ、受信者Ｂ、電子メール管理者の公開鍵を取得することになる。公開鍵の取得方法は、ここではとくに規定しない。取得した公開鍵は、暗号鍵暗号化部６７に渡される。

【００５４】暗号鍵暗号化部６７は、暗号鍵生成部６３で生成された前記暗号鍵を、公開鍵取得部６６により渡された受信者の公開鍵、送信者の公開鍵、電子メール管理者の公開鍵を用いて、それぞれ公開鍵暗号方式により暗号化し、受信者用暗号鍵情報、送信者用暗号鍵情報、管理用暗号鍵情報を作成する（ステップＳ２７）。ここで生成された各暗号鍵情報は、暗号化電子メール構築部６８に渡される。

【００５５】暗号化電子メール構築部６８は、本文暗号化部６２より渡された暗号化された本文、暗号鍵暗号化部６７より渡された受信者用暗号鍵情報、送信者用暗号鍵情報、管理用暗号鍵情報、ヘッダ情報解析部６５より渡されたヘッダ情報を用いて、暗号化電子メール（７０）を構築して（ステップＳ２８）、出力する。

【００５６】図８は、図２の電子メール（２０）を上記のようにして暗号化した暗号化電子メール（７０）の構造を示す。暗号化電子メール（７０）は、送信者情報（７１）、受信者情報（７２）からなるヘッダ情報、受信者Ａ用暗号鍵情報（７３）、受信者Ｂ用暗号鍵情報（７４）、送信者Ｓ用暗号鍵情報（７５）、管理用暗号鍵情報（７６）からなる電子メール本文暗号鍵情報、そして暗号化本文（７７）からなる。

【００５７】このように、この実施の形態による暗号化電子メールにも、管理用暗号鍵情報が付加されるので、第１の実施の形態と同様、電子メールの送信者及び受信者以外の第三者が暗号化電子メールに関する情報管理を行うことができる。

【００５８】さらに、図８の暗号化電子メール（７０）は、図４の暗号化電子メール（３０）と相違し、受信者情報に暗号化電子メール管理者が加えられている。こうすることにより、電子メール管理者用の暗号鍵情報がつけられる。また、電子メールが電子メール管理者にも配送されることになり、暗号化電子メールのログ機能を自動的に行うこともできる。

【００５９】また、この実施の形態によれば、従来の暗号化電子メールの枠組を大きく変えることなく第三者による暗号化電子メールの情報管理を行うことができるという利点がある。

【００６０】ところで、この実施の形態の電子メール暗号化装置の電子メール暗号化処理の手順は、図７に示したものに限らず、種々変形することができる。図９には、電子メール暗号化装置６０による電子メール暗号化処理の手順の他の例を示す。図７の手順とは、処理の順番が異なっているだけである。すなわち、図７では、暗号化鍵を作成すると（ステップＳ２２）、まず、電子メール本文の暗号化を行なったが（ステップＳ２３）、図９では、電子メール本文の暗号化（ステップＳ４１）は、暗号化電子メールフォーマットの構築の直前に行なっている（ステップＳ４２）。また、図７では、送信者の判別と受信者の判別（ステップＳ２５）をまとめて行ない、送信者用公開鍵の取得と受信者用公開鍵の取得（ステップＳ２６）をまとめて行ない、各公開鍵による本文の暗号鍵の暗号化（ステップＳ２７）をまとめて行なっているが、図９では、まず、送信者について、判別（ステップＳ３５）、送信者用公開鍵の取得（ステップＳ３６）、公開鍵による本文の暗号鍵の暗号化（ステップＳ３７）を行ない、次に、受信者について、判別（ステップＳ３９）、送信者用公開鍵の取得（ステップＳ４０）、公開鍵による本文の暗号鍵の暗号化（ステップＳ３７）を行なっている。

【００６１】また、これの他にも、種々の処理手順が考えられるが、当業者であれば容易に修正を施すことができるので、さらなる他の手順の例を一つ一つ説明することは省略する。

【００６２】この実施の形態の電子メール暗号化装置は、ハードウェアで実現することも可能であり、また、上記のような処理内容に相当するプログラムを作成し、これをコンピュータにインストールして実行させる形で実現することも可能である。

【００６３】次に、図１０に、本発明の第３の実施の形態に係る電子メール暗号化装置の基本構成を示す。この電子メール暗号化装置８０は、情報分離部８１、本文暗号化部８２、暗号鍵生成部８３、管理用ヘッダ情報付加部８４、ヘッダ情報解析部８５、公開鍵取得部８６、暗号鍵暗号化部８７、暗号化電子メール構築部８８を備えている。図１０の各部分は、基本的には、図６の対応する部分と同様のものである。ただし、この実施の形態では、第２の実施の形態と異なり、情報分離部８１で分離したヘッダ情報を暗号化電子メール構築部８８に与えている。

【００６４】また、図１８に示す従来の電子メール暗号化装置との違いは、情報分離部８１により分離されたヘッダ情報が、管理用ヘッダ情報付加部８４と暗号化電子メール構築部８８に渡される点である。

【００６５】この実施の形態の電子メール暗号化装置８０による電子メール暗号化処理の手順は、基本的には、図７や図９と同様である。もちろん、前述した実施の形態と同様に、図７や図９に示したものに限らず、種々変形することができる。

【００６６】この実施の形態が第２の実施の形態と異なるのは、情報分離部８１で分離したヘッダ情報を暗号化電子メール構築部８８に与えているので、ヘッダ情報解析部８５に渡される電子メールの受信者情報には電子メール管理者は含まれるが、暗号化電子メール構築部８８に渡される電子メール受信者情報には電子メール管理者は含まれない点にある。

【００６７】従って、この実施の形態によれば、図４と同様の暗号化電子メールを構築することができる。もちろん、この実施の形態による暗号化電子メールにも、管理用暗号鍵情報が付加されるので、第１，第２の実施の形態と同様、電子メールの送信者及び受信者以外の第三者が暗号化電子メールに関する情報管理を行うことができる。

【００６８】また、この実施の形態によれば、従来の暗号化電子メールの枠組を大きく変えることなく第三者による暗号化電子メールの情報管理を行うことができるという利点がある。

【００６９】もちろん、この実施の形態の電子メール暗号化装置は、ハードウェアで実現することも可能であり、また、上記のような処理内容に相当するプログラムを作成し、これをコンピュータにインストールして実行させる形で実現することも可能である。

【００７０】なお、第２の実施の形態で暗号化電子メールを構築する際に、ヘッダ情報の受信者情報から管理者

を削除するようにしても、図４と同様の暗号化電子メールを構築することができる。

【００７１】次に、図１１に、本発明の第４の実施の形態に係る電子メール転送装置を示す。この電子メール転送装置は、暗号化電子メールの転送を制限する機能を有するものである。この電子メール転送装置９０は、暗号化電子メール判別部９１、電子メール転送判断部９２、電子メール転送部９３を備えている。

【００７２】暗号化電子メールの転送の制限には、種々のものが考えられる。例えば、

①暗号化電子メールはすべて転送不可能とする。

②所定の条件を満たす暗号化電子メールのみ転送可能とする。例えば、暗号化電子メールの転送可能者リストを保有し、送信者がそのリストに載っているときのみ転送可能とする。

【００７３】図１２には、上記①の転送制限をする場合の転送処理手順の一例を示す。電子メール転送装置９０に入力された電子メールは、暗号化電子メール判別部９１により該電子メールが暗号化電子メールであるかどうかが判別される（ステップＳ５１）。その方法は様々であるが、例えば、暗号化電子メールの場合は、ヘッダ情報あるいは本文の一部に暗号化電子メールであることを示す情報が含まれるので、それが含まれるかどうかを検索することにより暗号化電子メールの判別を行う。暗号化電子メール判別部９１は、その結果を電子メール転送判断部９２に送る。

【００７４】電子メール転送判断部９２は、暗号化電子メール判別部９１の結果を基に該電子メールが転送可能かどうかの判断を行う。ここでは、暗号化電子メールでなければ転送可能とし（ステップＳ５２）、暗号化電子メールの場合は転送不可とする（ステップＳ５４）。

【００７５】転送可能と判断されたメールは、電子メール転送部９３に送られて転送される（ステップＳ５３）。電子メール転送部９３は、公知の電子メール転送方式と同様の機能を有し、ここでは機能の説明を省略する。

【００７６】図１３には、上記②の転送制限をする場合の転送処理手順の一例を示す。電子メール転送装置９０に入力された電子メールは、暗号化電子メール判別部９１により該電子メールが暗号化電子メールであるかどうかが判別される（ステップＳ６１）。その方法は様々であるが、例えば、暗号化電子メールの場合は、ヘッダ情報あるいは本文の一部に暗号化電子メールであることを示す情報が含まれるので、それが含まれるかどうかを検索することにより暗号化電子メールの判別を行う。暗号化電子メール判別部９１は、その結果を電子メール転送判断部９２に送る。

【００７７】電子メール転送判断部９２は、暗号化電子メール判別部９１の結果を基に該電子メールが転送可能かどうかの判断を行う。ここでは、暗号化電子メールの転送可能者リストを保有しているものとする。

【００７８】暗号化電子メールの場合は、転送可能とする（ステップＳ６１）。暗号化電子メールの場合は、電子メールのヘッダ情報の送信者情報を参照し、送信者がその転送可能者リストに載っている場合、転送可能とし（ステップＳ６４，Ｓ６２）、載っていない場合、転送不可とする（ステップＳ６４，Ｓ６５）。

【００７９】転送可能と判断されたメールは、電子メール転送部９３に送られて転送される（ステップＳ６３）。暗号化電子メールの転送の制限には、上記以外にも種々のものが考えられる。

【００８０】このように、この実施の形態によれば、暗号化電子メールに関する転送制御を行うことができる。

次に、図１４に、本発明の第５の実施の形態に係る電子メール転送装置を示す。この電子メール転送装置は、管理者用暗号鍵情報を含む暗号化電子メールは転送し、管理用暗号鍵情報を含まない暗号化電子メールは転送しない機能を有するものである。この電子メール転送装置１００は、暗号化電子メール判別部１０１、電子メール転送判断部１０２、電子メール転送部１０３、管理用暗号鍵情報検査部１０４を備えている。

【００８１】図１５には、この実施の形態の転送処理手順の一例を示す。電子メール転送装置１００に入力された電子メールは、暗号化電子メール判別部１０１により該電子メールが暗号化電子メールであるかどうかが判別される（ステップＳ７１）。その方法は、第４の実施の形態と同様、様々であるが、例えば、暗号化電子メールの場合は、ヘッダ情報あるいは本文の一部に暗号化電子メールであることを示す情報が含まれるので、それが含まれるかどうかを検索することにより暗号化電子メールの判別を行う。

【００８２】その結果が、暗号化電子メールである場合は、管理用暗号鍵情報検査部１０４により、該暗号化電子メールが管理用の暗号鍵情報を正しく含んでいるかどうかの検査を行う（ステップＳ７４）。その方法は様々であるが、例えば、暗号化電子メール内に管理用暗号鍵情報が含まれているかどうかを走査することにより検査することができる。また、管理用暗号鍵情報を含む暗号化電子メールのヘッダ情報に特別の識別子を含むようにしておけば、そのヘッダ情報を含むかどうかを検査する方法もある。

【００８３】暗号化電子メール判別部１０１は、管理用暗号鍵情報検査部１０４の出力を受け、その結果を電子メール転送判断部１０２に送る。電子メール転送判断部１０２は、暗号化電子メール判別部１０１の結果を基に、該電子メールが転送可能かどうかの判断を行う。暗号化電子メールでなければ転送可能とし（ステップＳ７２）、暗号化電子メールの場合は、管理用の暗号鍵情報を含んでいる暗号化電子メールの場合は転送を行い（ステップＳ７４、Ｓ７２）、含んでいない暗号化電子メー

ルの場合は転送を行わない（ステップＳ７４，Ｓ７５）。

【００８４】転送可能と判断されたメールは、電子メール転送部１０３に送られて転送される（ステップＳ７３）。電子メール転送部１０３は、公知の電子メール転送方式と同様の機能を有し、ここでは機能の説明を省略する。

【００８５】この実施の形態で述べた電子メール転送装置を、例えば、企業と外部との境界に設けることにより、管理用の暗号鍵情報を含まない暗号化電子メール、つまり電子メール管理者が情報管理を行うことができない暗号化電子メールを企業の外に出ないように設定することができる。

【００８６】次に、図１６に、本発明の第６の実施の形態に係る電子メール転送装置を示す。この電子メール転送装置は、管理用の暗号鍵情報を消去する機能を有するものである。この電子メール転送装置１１０は、暗号化電子メール判別部１１１、電子メール転送判断部１１２、電子メール転送部１１３、管理用暗号鍵情報検査部１１４、管理用暗号鍵情報除去部１１５を備えている。

【００８７】図１７には、この実施の形態の転送処理手順の一例を示す。電子メール転送装置１１０に入力された電子メールは、暗号化電子メール判別部１１１により該電子メールが暗号化電子メールであるかどうかが判別される（ステップＳ８１）。その方法は、第４の実施の形態と同様、様々であるが、例えば、暗号化電子メールの場合は、ヘッダ情報あるいは本文の一部に暗号化電子メールであることを示す情報が含まれるので、それが含まれるかどうかを検索することにより暗号化電子メールの判別を行う。

【００８８】その結果が、暗号化電子メールである場合は、管理用暗号鍵情報検査部１１４により、該暗号化電子メールが管理用の暗号鍵情報を正しく含んでいるかどうかの検査を行う（ステップＳ８４）。その方法は、前述の第５の実施の形態と同様とする。暗号化電子メール判別部１１１は、管理用暗号鍵情報検査部１１４の出力を受け、その結果を電子メール転送判断部１１２に送る。

【００８９】電子メール転送判断部１１２は、暗号化電子メール判別部１１１の結果を基に、該電子メールが転送可能かどうかの判断を行う。該電子メールが暗号化電子メールでなければ転送可能とし（ステップＳ８２）、電子メール転送部１１３に送る。該電子メールが暗号化電子メールの場合は、管理用暗号鍵情報を含んでいない場合は転送不可とし（ステップＳ８４，Ｓ８５）、管理用暗号鍵情報を含んでいる場合は転送可能とする（ステップＳ８４．Ｓ８７）。転送可能と判断された暗号化電子メールは、管理用暗号鍵情報除去部１１５に送られる。

【００９０】管理用暗号鍵情報除去部１１５は、電子メール転送判断部１１２から送られてきた暗号化電子メールから管理用暗号鍵情報を取り除き（ステップＳ８６）、電子メール転送部１１３に送る。

【００９１】転送可能と判断されたメールは、電子メール転送部１１３に送られて転送される（ステップＳ８３）。電子メール転送部１１３は、公知の電子メール転送方式と同様の機能を有し、ここでは機能の説明を省略する。

【００９２】この実施の形態により、第１～第３の実施の形態（図１，図６，図１０）の電子メール暗号化装置にて付加された管理用暗号鍵情報を暗号化電子メールから取り除くことができる。管理用暗号鍵情報は、ある組織内の情報管理にのみ必要なものであり、送信者と受信者にとっては、本来不必要な情報である。したがって、この実施の形態の電子メール転送装置を用いることにより、余分な管理用の情報を削除することができる。本発明は、上述した実施の形態に限定されるものではなく、その技術的範囲において種々変形して実施することができる。

【００９３】

【発明の効果】本発明（請求項１）によれば、電子メール本文の暗号化に用いた暗号鍵を電子メールの受信者と送信者以外の第三者の公開鍵により暗号化し、電子メールに付加するので、当該暗号化電子メールを受信者および送信者以外のて第三者も復号することができる。

【００９４】従って、第三者の公開鍵を電子メール情報管理者用のものにすれば、該管理者は電子メールの内容検査などの情報管理を行うことができる。本発明（請求項２）によれば、入力された電子メールの種類を判別し、その結果に応じて該電子メールの転送の可否を判断するので、電子メールの種類に応じた電子メールの転送の可否を判断基準を適宜設定することにより、電子メールの転送制御を行なうことができる。

【００９５】本発明（請求項３）によれば、上記発明（請求項２）の電子メール転送装置において、管理用の暗号鍵情報を含む暗号化電子メールから該暗号鍵情報を取り除く手段をさらに設けたので、メール送信者と受信者にとって本来不要である管理用の暗号鍵情報を除去することができる。

【図面の簡単な説明】

【図１】本発明の第１の実施の形態に係る電子メール暗号化装置の基本構成を示す図

【図２】電子メールの基本的構造を示す図

【図３】同実施の形態の電子メール暗号化処理の手順の一例を示すフローチャート

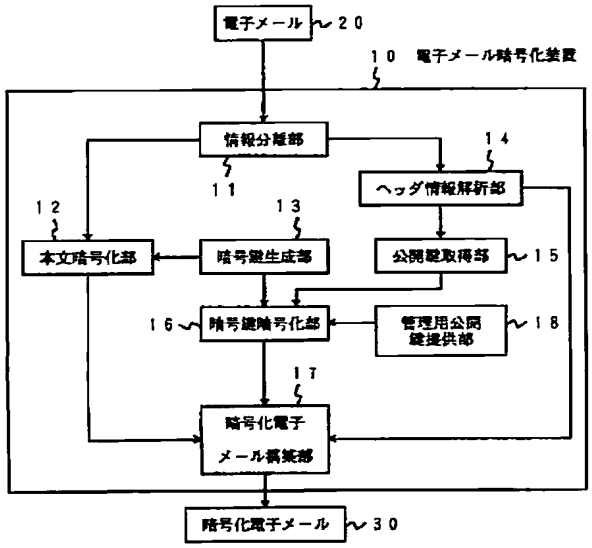
【図４】同実施の形態に係る電子メール暗号化装置から出力される暗号化電子メールの構造を示す図

【図５】同実施の形態の電子メール暗号化処理の手順の他の例を示すフローチャート

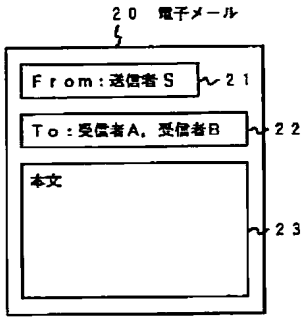
【図６】本発明の第２の実施の形態に係る電子メール暗

号化装置の基本構成を示す図
【図７】同実施の形態の電子メール暗号化処理の手順の一例を示すフローチャート
【図８】同実施の形態に係る電子メール暗号化装置から出力される暗号化電子メールの構造を示す図
【図９】同実施の形態の電子メール暗号化処理の手順の他の例を示すフローチャート
【図１０】本発明の第３の実施の形態に係る電子メール暗号化装置の基本構成を示す図
【図１１】同第４の実施の形態に係る電子メール転送装置の基本構成を示す図
【図１２】同実施の形態の転送処理手順の一例を示すフローチャート
【図１３】同実施の形態の転送処理手順の他の例を示すフローチャート
【図１４】同第５の実施の形態に係る電子メール転送装置の基本構成を示す図
【図１５】同実施の形態の転送処理手順の一例を示すフローチャート
【図１６】同第６の実施の形態に係る電子メール転送装置の基本構成を示す図
【図１７】同実施の形態の転送処理手順の一例を示すフローチャート
【図１８】従来の電子メール暗号化装置の基本構成を示す図
【図１９】従来の電子メール暗号化装置による暗号化電子メールの構造を示す図
【符号の説明】
１０，６０，８０…電子メール暗号化装置、１１，６１，８１…情報分離部、１２，６２，８２…本文暗号化部、１３，６３，８３…暗号鍵生成部、６４，８４…管理用ヘッダ情報付加部、１４，６５，８５…ヘッダ情報解析部、１５、６６，８６…公開鍵取得部、１６，６７，８７…暗号鍵暗号化部、１７，６８，８８…暗号化電子メール構築部、１８…管理用公開鍵提供部、９０，１００，１１０…電子メール転送装置、９１，１０１，１１１…暗号化電子メール判別部、９２，１０２，１１２…電子メール転送判断部、９３，１０３，１１３…電子メール転送部、１０４，１１４…管理用暗号鍵情報検査部、１１５…管理用暗号鍵情報除去部

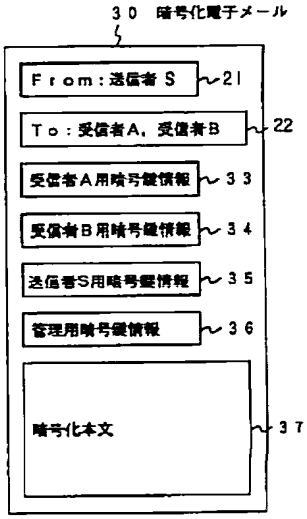
【図１】



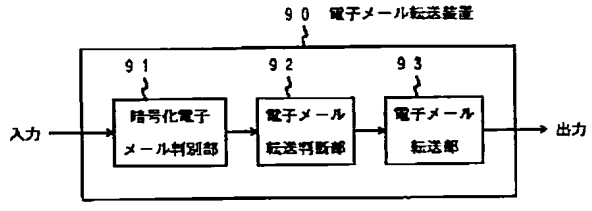
【図２】



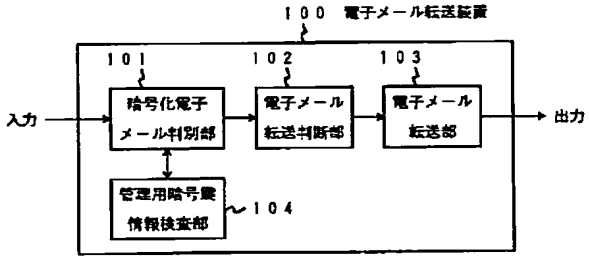
【図４】



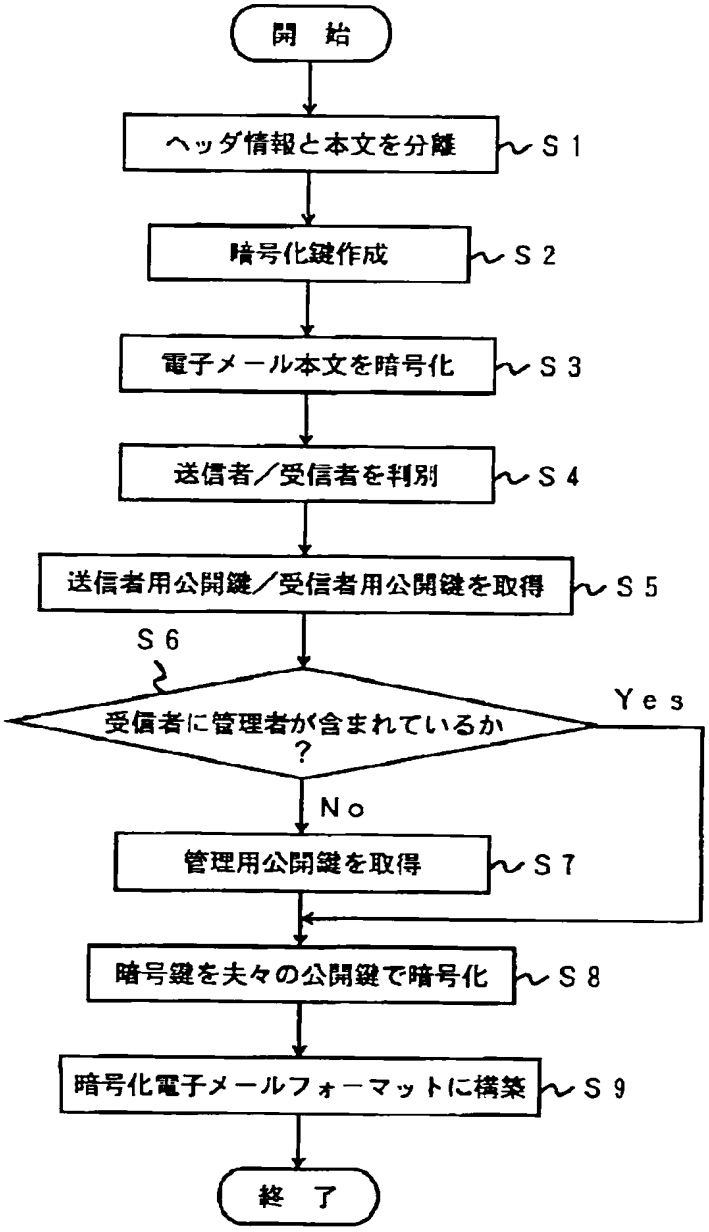
【図１１】



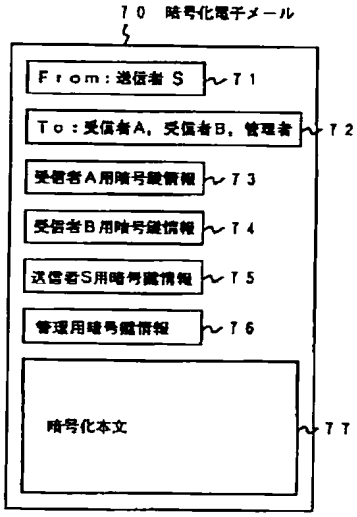
【図１４】



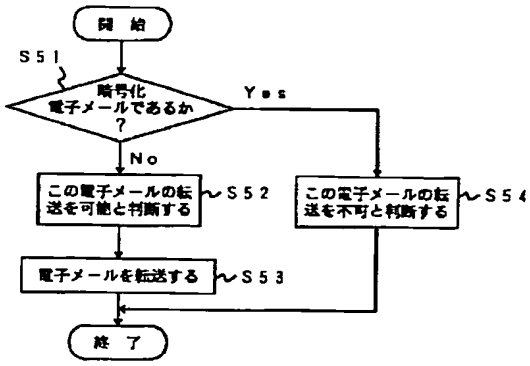
【図３】


開　始
ヘッダ情報と本文を分離
S１
暗号化鍵作成
S２
電子メール本文を暗号化
S３
送信者／受信者を判別
S４
送信者用公開鍵／受信者用公開鍵を取得
S５
S６
受信者に管理者が含まれているか？
Ｙｅｓ
Ｎｏ
管理用公開鍵を取得
S７
暗号鍵を夫々の公開鍵で暗号化
S８
暗号化電子メールフォーマットに構築
S９
終　了

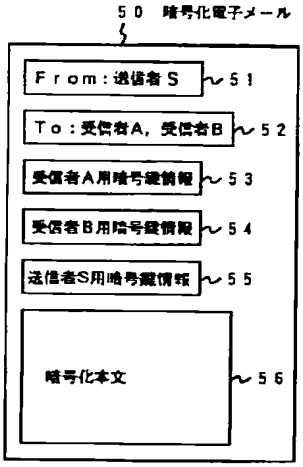
【図８】


７０　暗号化電子メール
Ｆｒｏｍ：送信者Ｓ
７１
Ｔｏ：受信者Ａ，受信者Ｂ，管理者
７２
受信者Ａ用暗号鍵情報
７３
受信者Ｂ用暗号鍵情報
７４
送信者Ｓ用暗号鍵情報
７５
管理用暗号鍵情報
７６
暗号化本文
７７

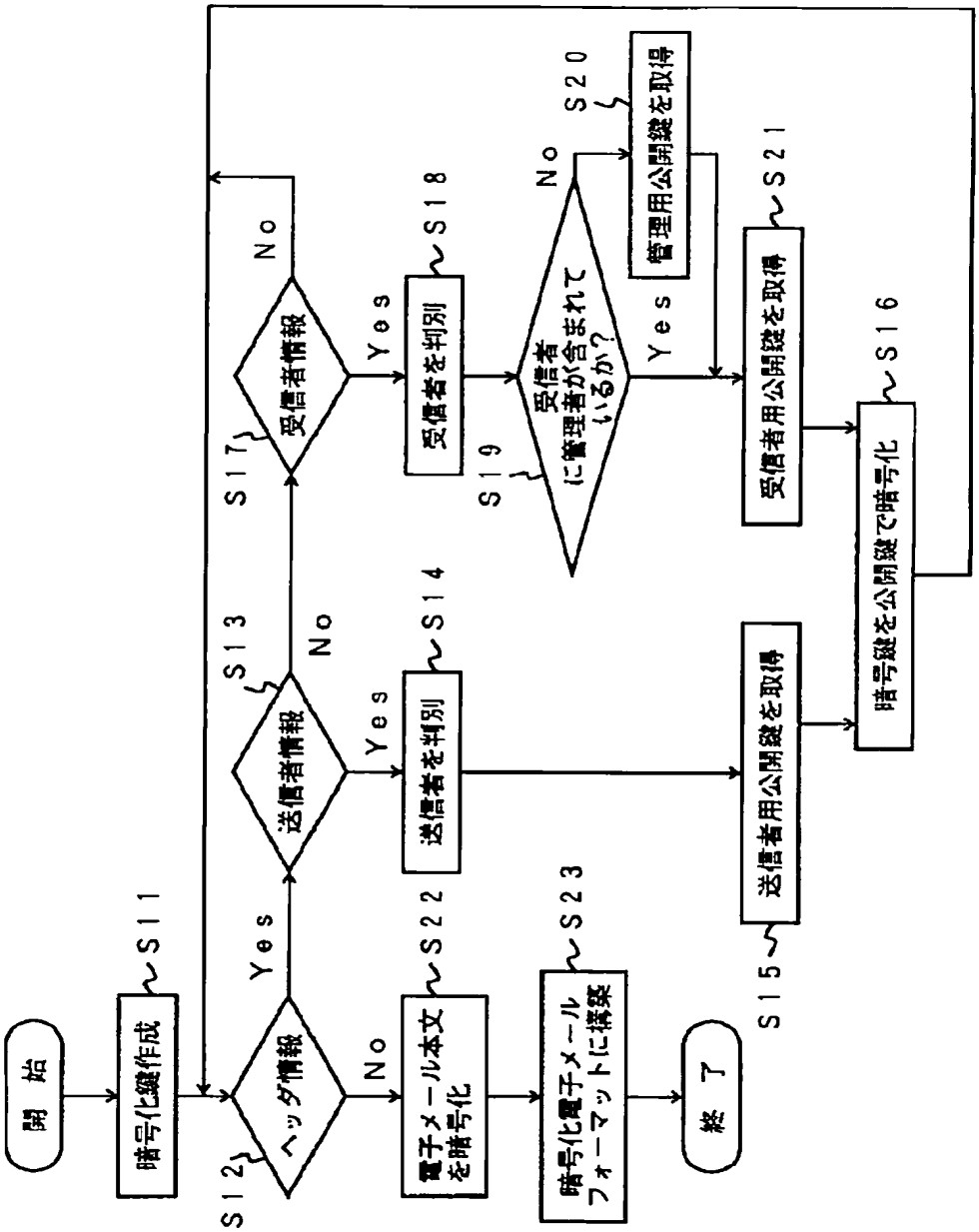
【図１２】


開　始
S５１
暗号化電子メールであるか？
Ｙｅｓ
Ｎｏ
この電子メールの転送を可能と判断する
S５２
この電子メールの転送を不可と判断する
S５４
電子メールを転送する
S５３
終　了

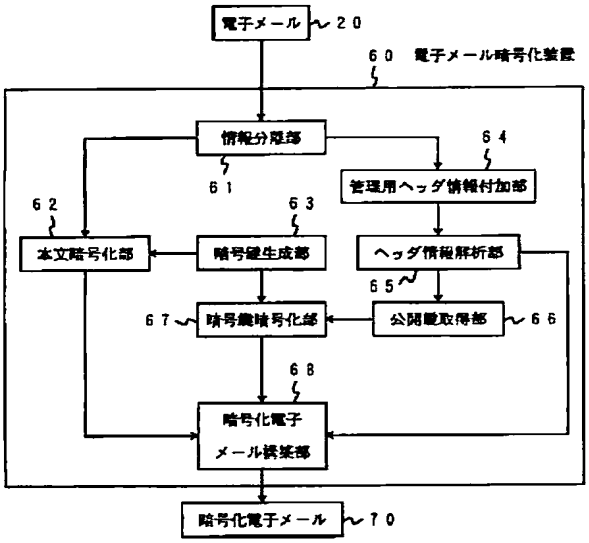
【図１９】


５０　暗号化電子メール
Ｆｒｏｍ：送信者Ｓ
５１
Ｔｏ：受信者Ａ，受信者Ｂ
５２
受信者Ａ用暗号鍵情報
５３
受信者Ｂ用暗号鍵情報
５４
送信者Ｓ用暗号鍵情報
５５
暗号化本文
５６

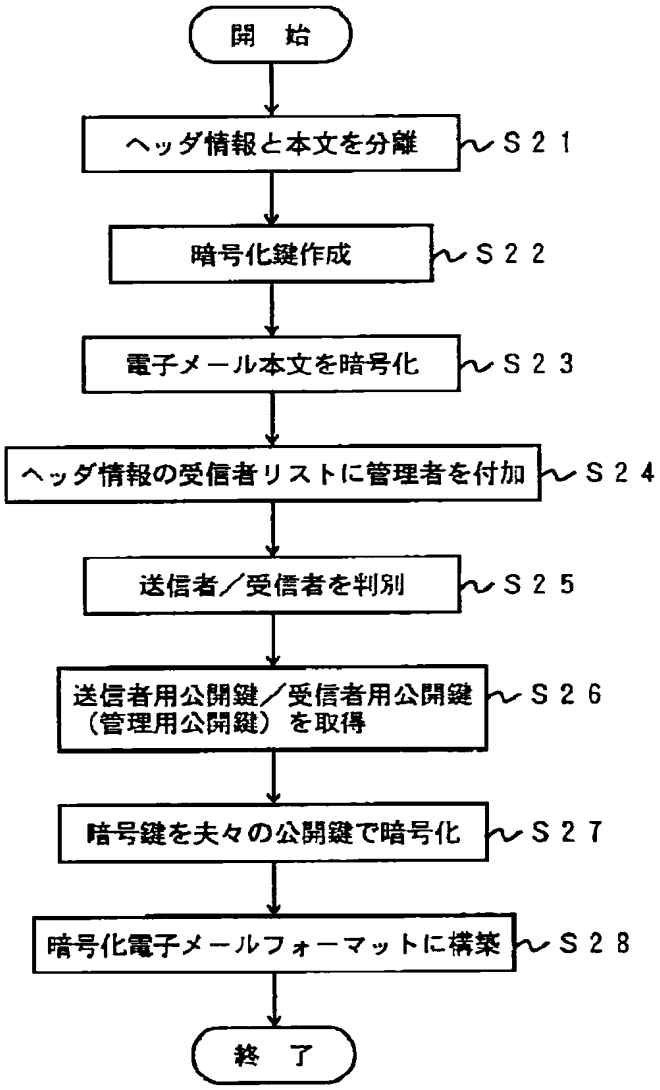
【図５】


開始
暗号化鍵作成
S11
ヘッダ情報
S12
Yes
No
送信者情報
S13
Yes
No
受信者情報
S17
Yes
No
電子メール本文を暗号化
S22
送信者を判別
S14
受信者を判別
S18
受信者に管理者が含まれているか？
S19
No
Yes
管理用公開鍵を取得
S20
暗号化電子メールフォーマットに構築
S23
送信者用公開鍵を取得
S15
受信者用公開鍵を取得
S21
暗号鍵を公開鍵で暗号化
S16
終了

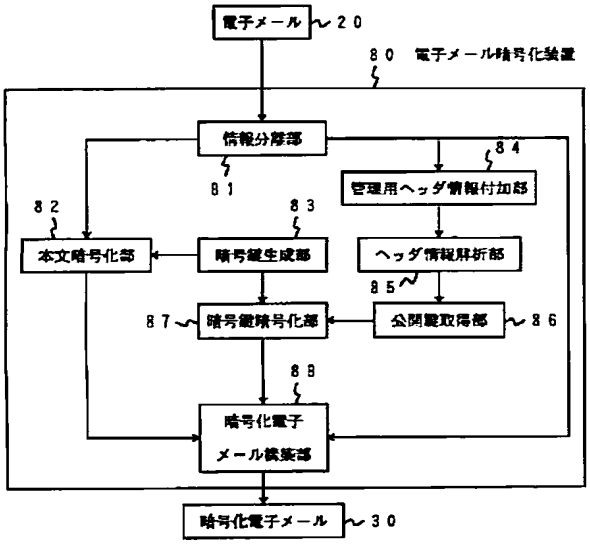
【図６】


電子メール
２０
６０　電子メール暗号化装置
情報分離部
６１
６４
管理用ヘッダ情報付加部
６２
６３
本文暗号化部
暗号鍵生成部
ヘッダ情報解析部
６５
６７
暗号鍵暗号化部
公開鍵取得部
６６
６８
暗号化電子
メール構築部
暗号化電子メール
７０

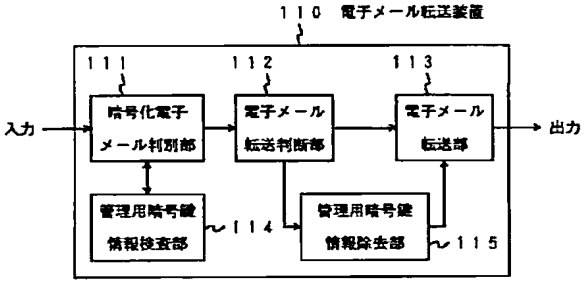
【図７】


開　始
ヘッダ情報と本文を分離
Ｓ２１
暗号化鍵作成
Ｓ２２
電子メール本文を暗号化
Ｓ２３
ヘッダ情報の受信者リストに管理者を付加
Ｓ２４
送信者／受信者を判別
Ｓ２５
送信者用公開鍵／受信者用公開鍵
（管理用公開鍵）を取得
Ｓ２６
暗号鍵を夫々の公開鍵で暗号化
Ｓ２７
暗号化電子メールフォーマットに構築
Ｓ２８
終　了

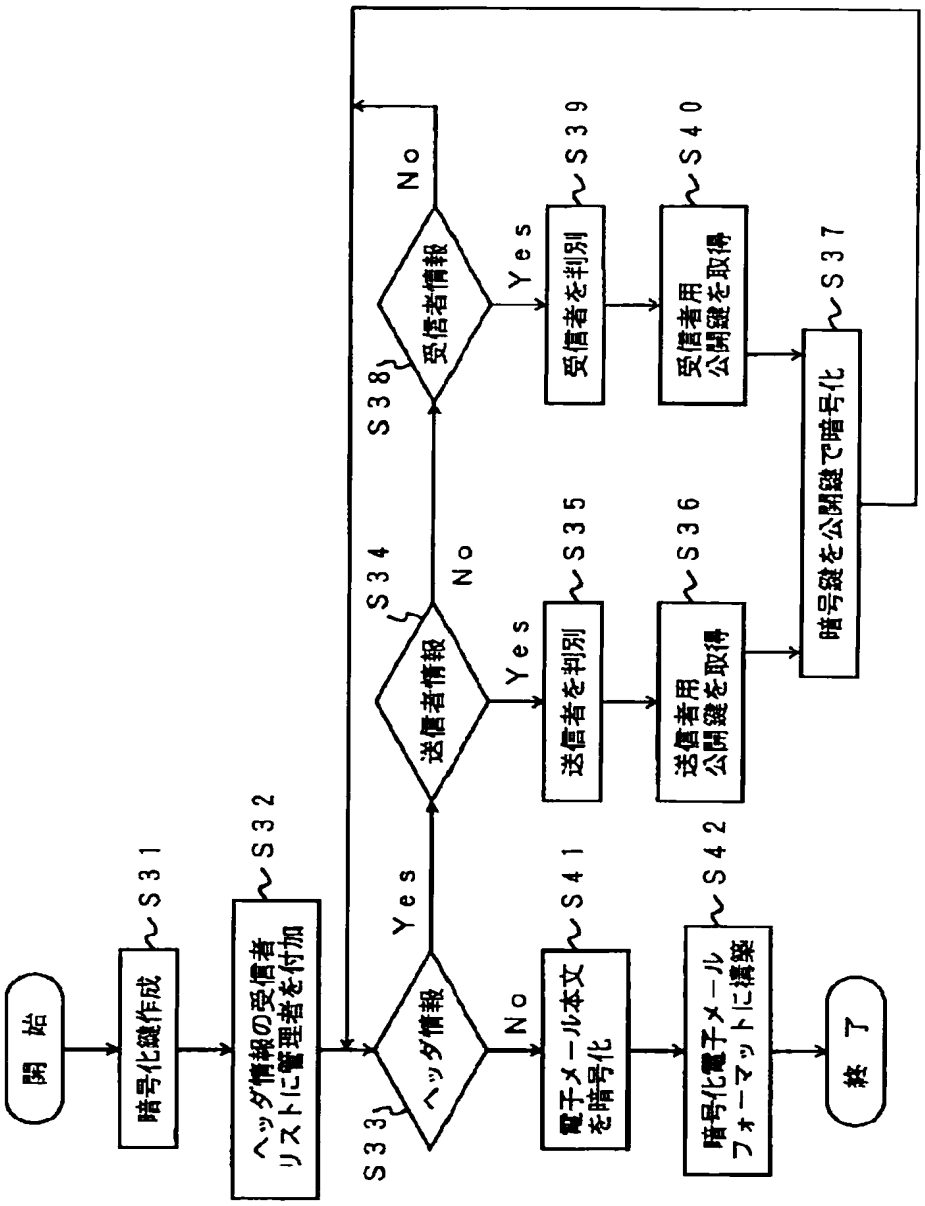
【図１０】


電子メール
２０
８０　電子メール暗号化装置
情報分離部
８１
８４
管理用ヘッダ情報付加部
８２
８３
本文暗号化部
暗号鍵生成部
ヘッダ情報解析部
８５
８７
暗号鍵暗号化部
公開鍵取得部
８６
８８
暗号化電子
メール構築部
暗号化電子メール
３０

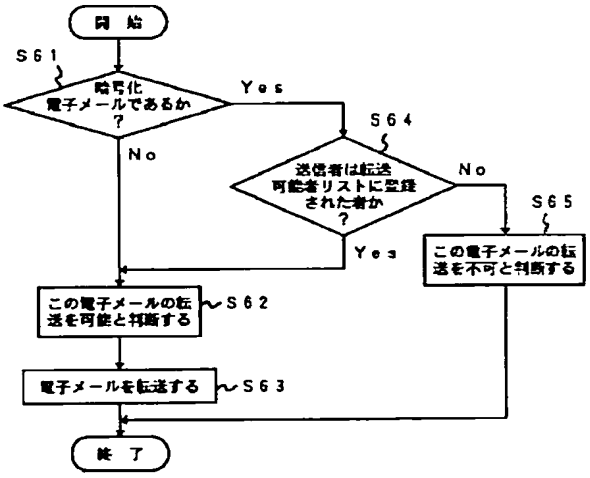
【図１６】


１１０　電子メール転送装置
１１１
１１２
１１３
入力
暗号化電子
メール判別部
電子メール
転送判断部
電子メール
転送部
出力
管理用暗号鍵
情報検査部
１１４
管理用暗号鍵
情報除去部
１１５

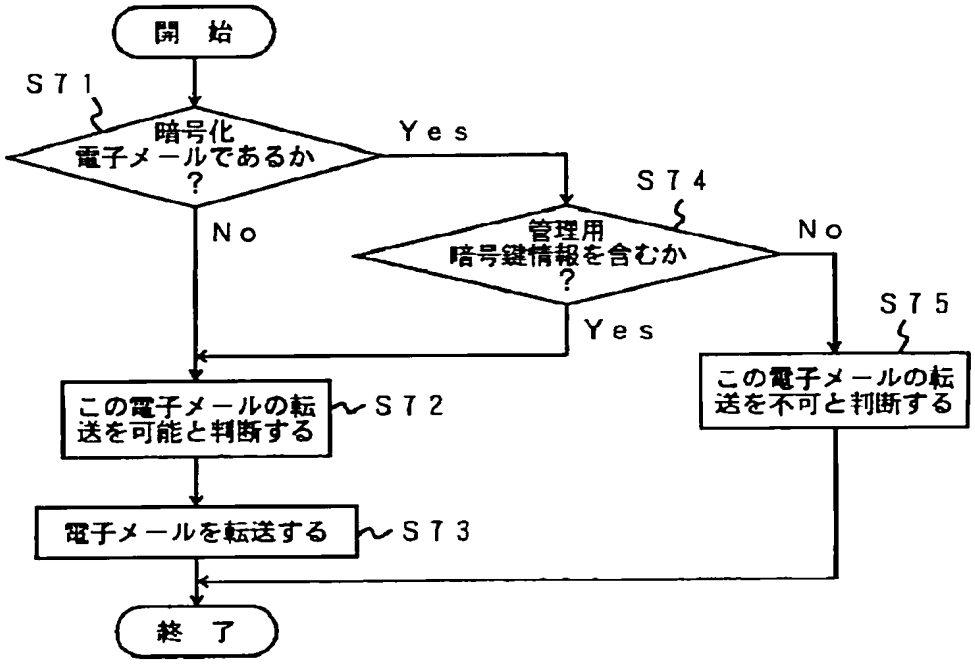
【図９】


開　始
暗号化鍵作成
S31
ヘッダ情報の受信者
リストに管理者を付加
S32
ヘッダ情報
S33
Yes
No
電子メール本文
を暗号化
S41
暗号化電子メール
フォーマットに構築
S42
終　了
送信者情報
S34
Yes
No
送信者を判別
S35
送信者用
公開鍵を取得
S36
受信者情報
S38
Yes
No
受信者を判別
S39
受信者用
公開鍵を取得
S40
暗号鍵を公開鍵で暗号化
S37

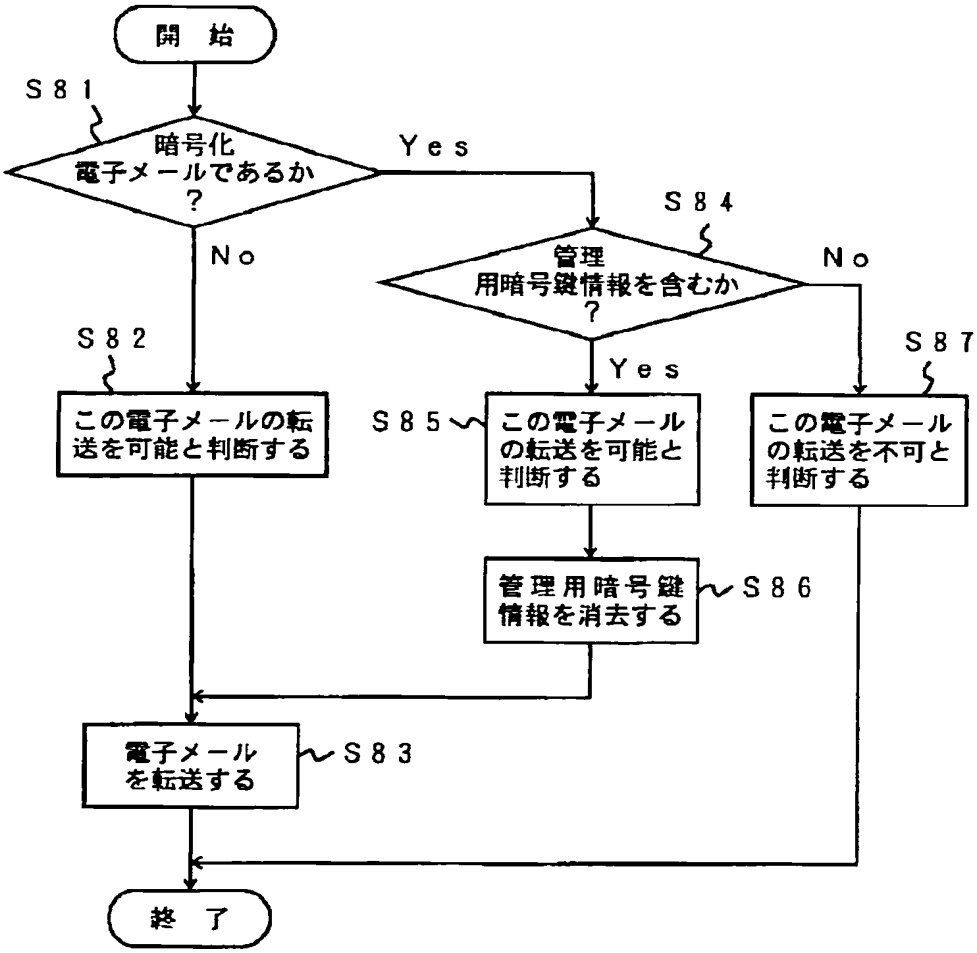
【図１３】


開　始
S61
暗号化
電子メールであるか
？
Yes
No
S64
送信者は転送
可能者リストに登録
された者か
？
No
Yes
S65
この電子メールの転
送を不可と判断する
この電子メールの転
送を可能と判断する
S62
電子メールを転送する
S63
終　了

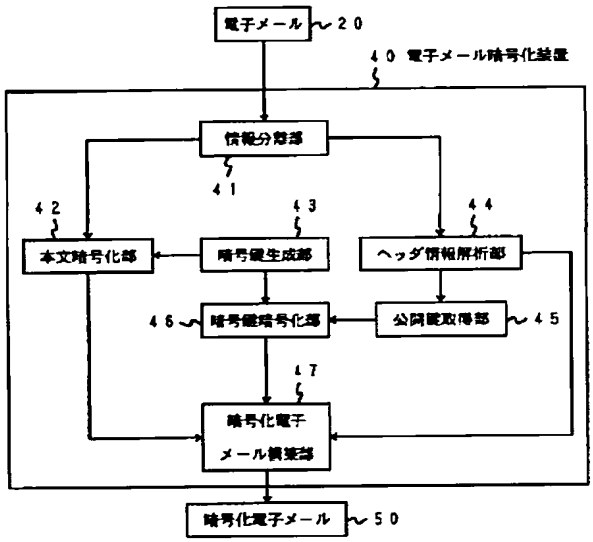
【図１５】


開　始
S71
暗号化
電子メールであるか
？
Yes
No
S74
管理用
暗号鍵情報を含むか
？
No
Yes
S75
この電子メールの転
送を不可と判断する
この電子メールの転
送を可能と判断する
S72
電子メールを転送する
S73
終　了

【図１７】


開　始
S８１
暗号化
電子メールであるか
？
Ｙｅｓ
Ｎｏ
S８４
管理
用暗号鍵情報を含むか
？
Ｎｏ
Ｙｅｓ
S８２
この電子メールの転送を可能と判断する
S８５
この電子メールの転送を可能と判断する
S８７
この電子メールの転送を不可と判断する
管理用暗号鍵情報を消去する
S８６
電子メールを転送する
S８３
終　了

【図１８】



フロントページの続き

(51) Int.Cl.[6]		識別記号	庁内整理番号	Ｆ Ｉ		技術表示箇所
Ｈ０４Ｌ	12/54			Ｈ０４Ｌ 9/00	６０１Ｅ	
	12/58		9466－5K	11/20	１０１Ｂ	